UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION

UNITED STATES OF AMERICA,	:	**CASE NO.** 1:21CR-130
Plaintiff,	:	
	:	**JUDGE** J. BLACK
v.	:	
	:	
GEORGIAN GOREA	:	**INDICTMENT**
	:	
	:	**18 U.S.C. § 1029(b)(2)**
Defendant.	:	**18 U.S.C. § 1349**

THE GRAND JURY CHARGES:

COUNT ONE
(Conspiracy to Commit Bank Fraud)

1. At all times material to the Indictment, Financial Institution-1 was a financial institution operating within the Southern District of Ohio, insured by the Federal Deposit Insurance Corporation, and engaged in banking activities that affect interstate commerce.
2. At all times material to the Indictment, Financial Institution-2 was a financial institution operating within the Southern District of Ohio, insured by the Federal Deposit Insurance Corporation, and engaged in banking activities that affect interstate commerce.
3. Beginning on or about August 2019 and continuing to on or about September 29, 2019, in the Southern District of Ohio and elsewhere, the defendant, **GEORGIAN GOREA (GOREA)**, conspired with others, both known and unknown to the Grand Jury, to commit the offense of bank fraud, that is, to knowingly execute or attempt to execute a scheme or artifice to (1) defraud a financial institution, or (2) obtain moneys, funds or property owned by, or under the custody or control of a financial institution by means of false or fraudulent pretenses, representations, or promises, in violation of 18 U.S.C. § 1344.
4. The purpose of the conspiracy was to fraudulently obtain debit card and credit card information by installing skimming devices on automatic teller machines (ATMs), use such

stolen information to create re-encoded debit or credit cards, and then fraudulently withdraw funds from the compromised accounts of bank customers using the re-encoded debit or credit cards. Specifically, as part of the conspiracy, defendant **GOREA** placed "skimming" devices on the ATMs of Financial Institution-1 in the Southern District of Ohio and elsewhere and used the information obtained from the skimming devices to conduct cash withdrawals at ATMs of Financial Institution-2 in the Southern District of Ohio and elsewhere.

5. As to the manner and means, the skimmer devices fraudulently obtained bank account information from credit cards and debit cards that were inserted in the ATMs by unwitting customers. The stolen account information was used to create "re-encoded" credit cards. The co-conspirators then stole and fraudulently withdrew funds from the compromised bank accounts at Financial Institution 1 through ATMs using the re-encoded cards. When installing a skimming device, co-conspirators typically also installed a camera facing the pin pad of the ATM in order to capture the PIN numbers entered by customers.

6. The specific acts within the conspiracy include the following:

   a. A skimmer was installed on ATM-1 of Financial Institution-1 by the co-conspirators in the Southern District of Ohio on August 7, 2019. **GOREA** was one of the individuals involved in the physical installation of the skimmer on ATM-1 on August 7, 2019. The skimmer was removed by the coconspirators on or about August 11, 2019.

   b. Financial Institution-1 identified approximately 342 debit card numbers that were compromised as a result of the skimming device installed on ATM-1 from August 7, 2019, to August 11, 2019. This list included the locations of any "cash out" attempts conducted using the compromised card numbers.

   c. The stolen account information from ATM-1 was used to attempt withdrawals or "cash-outs" of the compromised accounts at ATMs of Financial Institution-2.

d. ATM photos from Financial Institution-2 showed **GOREA** and other coconspirators using the compromised card numbers (from Financial Institution-1 ATM) to conduct cash withdrawals at approximately 16 ATMs of Financial Institution-2. These 16 ATMs were located in the Southern District of Ohio, with the majority located in the Cincinnati metropolitan area.

7. A review of Financial Institution-2's ATM camera photos combined with a review of the compromised card numbers provided by Financial Institution-1, revealed that **GOREA** and others used the compromised card numbers obtained from the skimming device previously installed on ATM-1 to conduct their cash out transactions between approximately August 31, 2019 and September 3, 2019.

8. Another skimming device was installed and removed at Financial Institution-1's ATM located in Celina, Ohio (ATM-2) by the co-conspirators. Specifically, on or about September 28, 2019, at approximately 7:15am, **GOREA** arrived at ATM-2 in a Toyota sport utility vehicle and installed an electronic device into ATM-2's card reader.

9. On September 29, 2019, **GOREA** approached the ATM in a dark color Toyota sport utility vehicle. **GOREA** proceeded to remove a black bar from beneath the face of ATM and departed.

10. The actions of **GOREA** and his coconspirators defraud Financial Institution-1 and other financial institutions of funds and caused actual losses.

All in violation of Title 18, United States Code, Section 1349.

COUNT TWO
(Conspiracy to Commit Access Device Fraud)

11. Paragraphs 1-2 and 4-10 are incorporated as if fully restated herein.

12. Beginning on or about August 2019 and continuing to on or about September 29, 2019, in the Southern District of Ohio, the defendant, **GEORGIAN GOREA**, did conspire with others, known and unknown to the grand jury, to commit access device fraud in violation

of 18 U.S.C. § 1029(a)(2) (use of an unauthorized access device) and 18 U.S.C. § 1029(a)(3) (possession of 15 or more unauthorized access devices).

All in violation of Title 18, United States Code, Section 1029(b)(2).

A TRUE BILL.

/s/
GRAND JURY FOREPERSON

KENNETH L. PARKER
UNITED STATES ATTORNEY

TIMOTHY S. MANGAN
ASSISTANT UNITED STATES ATTORNEY

EG